GRAINGER
FOR THE ONES WHO GET IT DONE

100 Grainger Parkway
Lake Forest, IL 60045-5201
Tel: 847.535.1000
Fax: 847.535.9243
www.grainger.com

April 17, 2018

To: U.S. State Attorney General and
Consumer Protection Office Distribution List

Re: Notice of Data Breach

Dear Sir or Ma'am:

W.W. Grainger, Inc. is a B2B provider of MRO (maintenance, repair and operations) supplies, headquartered in Lake Forest, IL. At Grainger, we take privacy and security very seriously, including prompt response to security incidents. I am writing to inform you of a recent matter involving Grainger's third-party service provider [24]7.ai, which may have affected the personal information of individuals who are resident in your state (see Exhibit A).

As was widely reported in the news, [24]7.ai is an online chat service provider to many companies in the marketplace. On April 10, 2018, Grainger was notified by [24]7.ai that [24]7.ai was involved in a cyber incident, which occurred from September 26, 2017 through October 12, 2017. During this time frame, credit card information of those conducting business with certain [24]7.ai corporate clients, including Grainger, may have been accessed, as well as card security codes, expiration dates, and cardholder names and addresses. Importantly, this matter does not involve any malware or security vulnerability associated with Grainger's systems. Rather, those customers who manually entered credit card information at the point of purchase on Grainger.com or its mobile app may have been affected by malware on [24]7.ai's systems that allowed for such information to be potentially collected by an unauthorized party.

Upon being notified by [24]7.ai, Grainger immediately launched an investigation with the assistance of cybersecurity counsel and outside forensics experts. We have notified law enforcement, our acquiring bank, and the credit card brands. We have also communicated regularly with [24]7.ai regarding this matter, and have been provided assurances from [24]7.ai that this matter was resolved as of October 12, 2017. In further response to this matter, we are reviewing our security-related diligence, contractual arrangements, and vendor management processes with respect to both [24]7.ai specifically, and more generally as well.

While we have no evidence of unauthorized transactions or fraud attributable to the [24]7.ai matter, out of an abundance of caution, Grainger is offering 12 months of complimentary identity protection and 12 months of complimentary credit monitoring services through Kroll. Information about these services is contained in the separately attached template notification letter, which we plan to send to all potentially affected individuals during the latter part of this week.

If you have any questions, please do not hesitate to call me at (847) 535-1047 or email at aimee.nolan@grainger.com.

Respectfully submitted,

Aimee M Nolan

Aimee Nolan
Associate General Counsel and Chief Intellectual Property Counsel

Attachments

Exhibit A

Approximate number of potentially affected residents in New Hampshire: 120

<Template Individual Notification>

Re: Notice of Third-Party Data Breach

Dear Grainger Customer,

We are contacting our customers who may have entered their credit card information to make a purchase on Grainger's website or mobile app between September 26, 2017 and October 12, 2017. Grainger learned last week that the company it works with to provide its online chat service, [24]7.ai, had a security breach that might have allowed access to your credit card information.

It is important to note that neither Grainger nor [24]7.ai have any evidence of unauthorized transactions or fraud attributable to this matter. However, given our commitment to customer service, we are providing this notice to all customers who might possibility be affected.

What Happened?

On April 10, 2018, Grainger was notified by [24]7.ai that [24]7.ai was involved in a cyber incident, which occurred from September 26, 2017 through October 12, 2017. During this time, credit card information of those conducting business with certain [24]7.ai clients, including Grainger, may have been accessed. Those customers who used guest check out and manually entered credit card information on Grainger.com or its app were potentially affected.

You have been identified as a Grainger customer affected by this [24]7.ai incident.

What Information Was Involved?

Information related to this incident includes credit card numbers, security codes, card expiration dates, names and addresses.

What Grainger is Doing.

Upon being notified by [24]7.ai of this incident, Grainger immediately began following its cybersecurity protocol by working with a leading cybersecurity expert to conduct its own investigation, alerting the credit card companies about the situation and affected cards, and notifying law enforcement officials. Grainger also communicated regularly with [24]7.ai. In connection with the foregoing, Grainger received assurances from [24]7.ai that the incident was resolved as of October 12, 2017.

While we cannot definitively determine whether any of our customers' information was actually accessed or subsequently compromised, Grainger is offering you the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, a Current Credit Report, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **<<IDMonitoringURL>>** to activate and take advantage of your identity monitoring services.
*You have until **<<Date>>** to activate your identity monitoring services. You can use these services at any time during the next 12 months.*

What You Can Do.

We urge you to remain vigilant against threats of identity theft or fraud, and to regularly review your credit card statements and credit reports for any unauthorized activity.

If you ever suspect that you are a victim of identity theft or fraud, you have the right to file a police report. You also may contact your State Attorney General's office or the Federal Trade Commission to learn about the steps you can take to protect yourself against identity theft. It's also a good practice to change all of your passwords on a regular basis and never use the same password for multiple system logins.

Additional information from [24]7.ai follows. We also encourage you to review the Tips & Resources below to learn more about credit and identity protection.

For More Information.

If you have questions or need additional information, please call Kroll toll free at 1-833-231-6259 from 8:00 AM to 5:00 PM CT, Monday through Friday, excluding major holidays.

We appreciate your business. The security and confidentiality of your information is our priority and something we take very seriously.

Sincerely,

Nadalie Bosse

Vice President, U.S. Contact Centers

[24]7.ai Issues Statement on Information Security

[24]7.ai discovered and contained an incident potentially affecting the online customer payment information of a small number of our client companies, and affected clients have been notified. The incident began on Sept. 26, and was discovered and contained on Oct. 12, 2017. We have notified law enforcement and are cooperating fully to ensure the protection of our clients and their customers' online safety. We are confident that the platform is secure, and we are working diligently with our clients to determine if any of their customer information was accessed.

About [24]7.ai

[24]7.ai is redefining the way companies interact with consumers. Using artificial intelligence and machine learning to understand consumer intent, the company's technology helps companies create a personalized, predictive and effortless customer experience across all channels. The world's largest and most recognizable brands are using intent-driven engagement from [24]7.ai to assist several hundred million visitors annually, through more than 1.5 billion conversations, most of which are automated. The result is an order of magnitude improvement in digital adoption, customer satisfaction, and revenue growth. For more information, visit: http://www.247.ai.

TIPS AND RESOURCES

What Government Agencies Provide Resources?

- *U.S. Federal Trade Commission (FTC):* The FTC has helpful information about how to avoid and protect against ID theft. Write to: Consumer Response Center, 600 Pennsylvania Ave., NW, H-130, Washington, D.C. 20580. Call Toll-Free: 1-877-IDTHEFT (438-4338); or Visit: http://www.ftc.gov/idtheft
- *State Attorney General Offices:* You may contact the Attorney General's office in the state in which you reside for more information about preventing and managing ID theft.

  For IOWA Residents: You may contact local law enforcement or the Iowa Attorney General's Office at 1305 E. Walnut St., Des Moines, IA 50319; Tel: (515) 281-5164; or http://www.iowa.gov/government/ag

  For MARYLAND Residents: You may obtain information about preventing identity theft from the FTC or the Maryland Attorney General's Office at 200 St. Paul Place, Baltimore, MD 21202; Tel: (888) 743-0023; or http://www.oag.state.md.us

  For NEW MEXICO Residents: You have a right to place a security freeze on your credit report or submit a declaration of removal with a consumer reporting agency pursuant to the Fair Credit Reporting and Identity Security Act. Please see below for more information on security freezes.

  For NORTH CAROLINA Residents: You may obtain information about preventing identity theft from the FTC or the North Carolina Attorney General's Office at 9001 Mail Service Center, Raleigh, NC 27699-9001; Tel: (919) 716-6400; Fax: (919) 716-6750; or http://www.ncdoj.com

  For RHODE ISLAND Residents: You may obtain information about preventing identity theft from the FTC or the Rhode Island Attorney General's Office at 150 South Main Street, Providence, RI 02903; Tel: (401) 274-4400; or http://www.riag.ri.gov

How Do I Get A Free Credit Report?

- You may obtain one (1) free copy of your credit report once every 12 months, and may purchase additional copies. Call Toll-Free: 1-877-322-8228; or Visit: https://www.annualcreditreport.com; or contact: Equifax, P.O. Box 740241, Atlanta, GA 30374-0241 (800) 685-1111 (www.equifax.com); Experian P.O. Box 2002, Allen, TX 75013, (888) 397-3742 (www.experian.com) TransUnion, P. O. Box 1000, Chester, PA 19022, (800) 888-4213 (www.transunion.com).

What is a "Fraud Alert"?

- You may have the right to place a fraud alert in your file to alert potential creditors that you may be a victim of identity theft. Creditors must then follow certain procedures to protect you. You should know that a fraud alert may delay your ability to obtain credit. An "initial fraud alert" stays in your file for at least 90 days. An "extended fraud alert" stays in your file for 7 years, and will require an identity theft report, which is usually a filed police report. You may place a fraud alert by calling any one of the three national consumer reporting agencies: Equifax: 1-800-525-6285; Experian: 1-888-397-3742; TransUnion: 1-800-680-7289

What is a "Security Freeze"?

- Certain U.S. state laws allow a security freeze, which prevents credit, loans or services from being approved in your name without your consent. A security freeze can interfere with or delay your ability to obtain credit.
- To place a freeze, send a request by mail to each consumer reporting agency (addresses below) with the following (for each individual): (1) Full name, middle initial and any suffixes; (2) Social Security Number; (3) Date of Birth; (4) proof of current address (such as a utility bill or telephone bill) and list of previous addresses for past five years; (5) copy of government issued ID card, and (6) copy of police report, investigative report or complaint to law enforcement regarding ID theft. You may be charged a fee up to $5.00 to place, lift, and/or remove a freeze, unless you are a victim of ID theft or the spouse of a victim, and you have submitted a valid police report relating to the ID theft incident to the consumer reporting agency. The consumer reporting agencies have three business days after receiving your letter to place a security freeze on your credit report.

The credit bureaus must also send written confirmation to you within five (5) business days and provide you a unique PIN or password that can be used by you to authorize the removal or lifting of the security freeze.

- To lift the security freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the consumer reporting agencies by mail and include proper identification (name, address, and SSN) and the PIN number or password provided to you when you placed the security freeze as well as the identities of entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The consumer reporting agencies have three business days after receiving your request to lift the security freeze for the identified entities or specified time period.
- To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and SSN) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three business days after receiving your request to remove the freeze. *Equifax Security Freeze*: P.O. Box 105788, Atlanta, Georgia 30348; *Experian Security Freeze*: P.O. Box 9554, Allen, TX 75013; *TransUnion (Fraud Victim Assistance Division)*: P.O. Box 6790, Fullerton, CA 92834-6790.